Security Policy

Version: 1.3

Document change

Version	Author	Date	Description
V1.0	Yi Xing	2020/3/4	Create
V1.1	Yi Xing	2020/5/29	Create
V1.2	Yi Xing	2020/6/11	Modified
V1.3	Yi Xing	2020/8/7	Modified

Table of content

Purpose

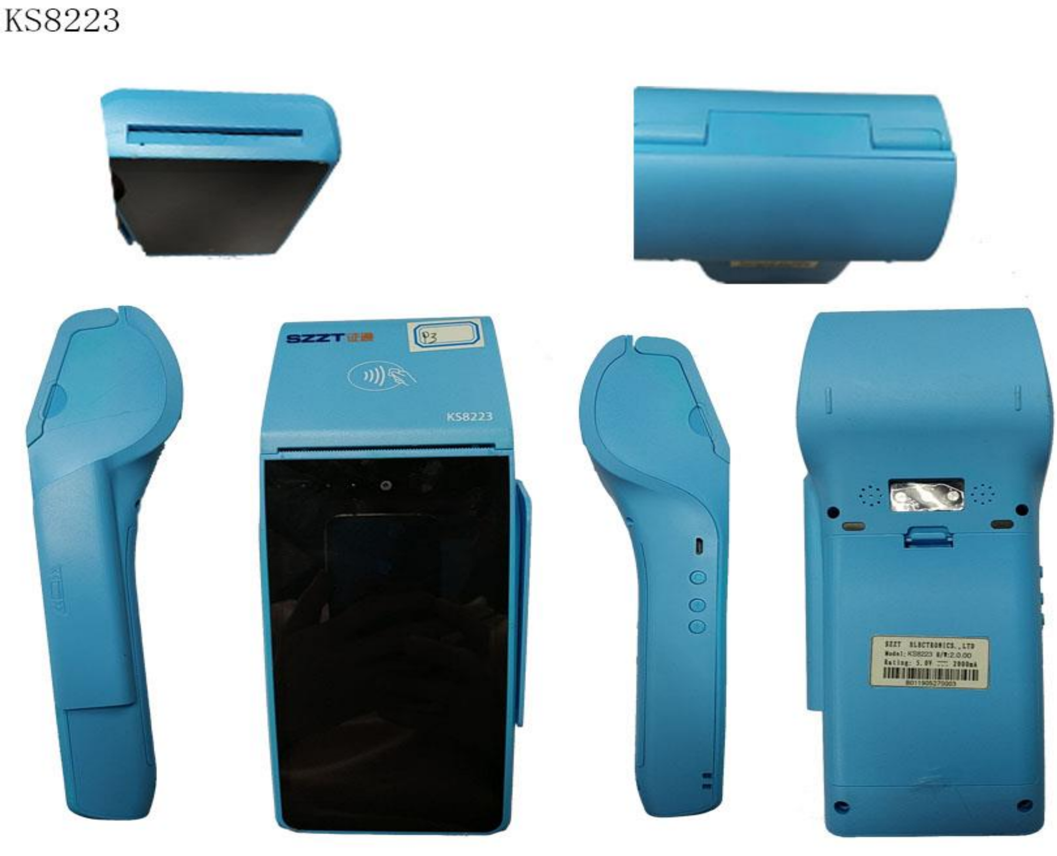
This document is provided for internal users, application developers, acquirers and end-users to refer before they use the device, so all relevant parties will know how to use the device in a secure way.

1. General Description

1.1. Product Name and Appearance

Product Name: KS8223

Appearance:



1.2. Product Type

The KS8223 has been PCI PTS approved as an attended handheld device, and does not require a privacy shield. The use of the device in an unattended environment or as a desktop device will violate the PCI PTS approval of the device.

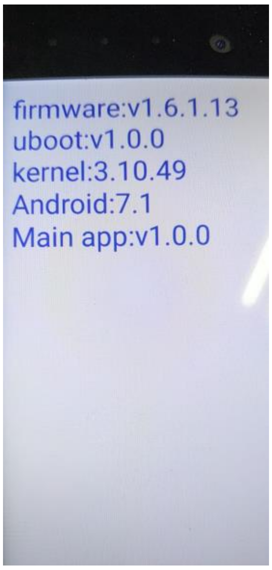
1.3. Identification

The KS8223 is a stand-alone PED terminal assessed for PTS POI v5.1. The KS8223 provides PIN entry and card readers.

To identify the device, please check the equipment according to the following steps:

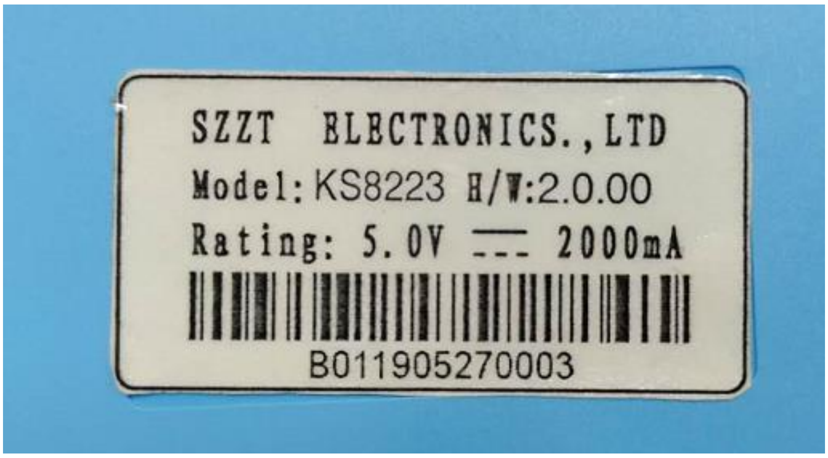
Check the device's software and hardware version, as shown in the picture below:

The software version can be checked after powering on the device, entering system menu and then pressing button "version".

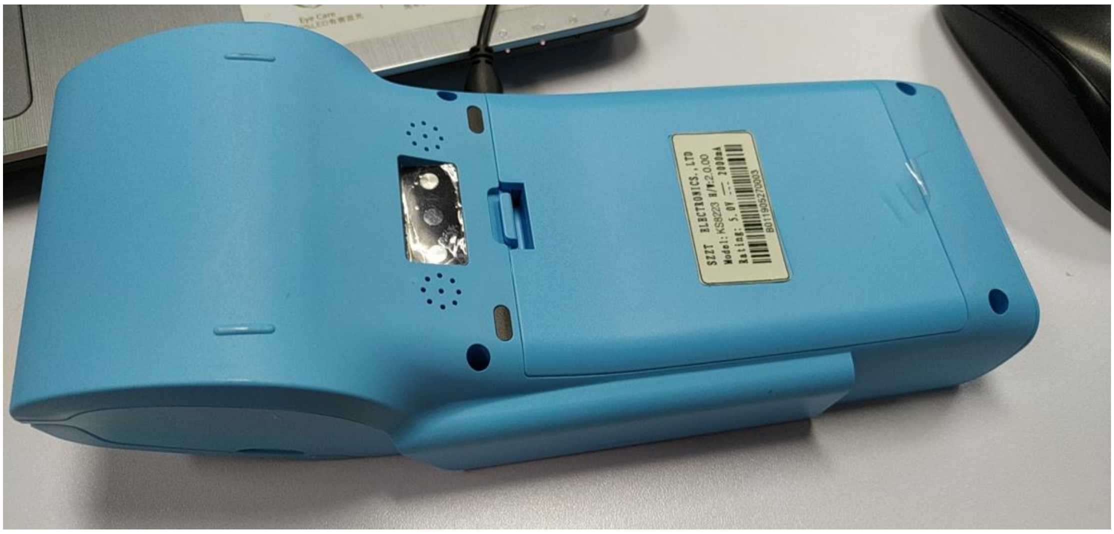


firmware:v1.6.1.13
uboot:v1.0.0
kernel:3.10.49
Android:7.1
Main app:v1.0.0

The hardware version could be found on the bottom of the device.



SZZT ELECTRONICS.,LTD
Model: KS8223 H/W:2.0.00
Rating: 5.0V ⎓ 2000mA
B011905270003



1.4. Device Functions

The KS8223 is a stand-alone POS terminal, which provides Touch Screen, IC Card Reader (ICCR), Magnetic Stripe Reader (MSR), LCD and thermal printer. It is designed for portable and handheld use, so that the device can be shielded by the body when in use. The power system is based on a DC 5.0V power supply or battery and the communications to the external world are based on WIFI, USB and Cellular(2G/3G/4G).

2. Installation and User Guidance

2.1 Initial Inspection

1. Check the packing, make sure it is intact. If it was broken or damaged, refuse to accept and sign, inform the express company to be responsible for the loss.

2. Check the tamper-evident label of each box with device, make sure the label is not ripped off or broken. If it was broken or damaged, open the box to check whether or not the device exists. Then refuse to accept and sign, inform the express company to be responsible for the loss, and ask the vendor if there is any product that has been opened and lost.

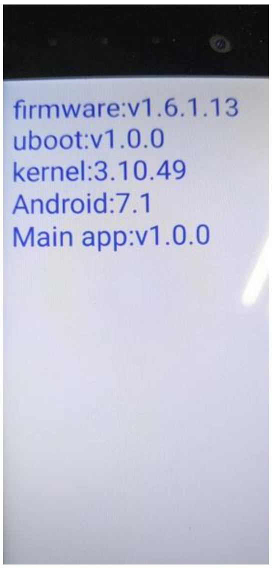
3. After ensuring the package of product is well, sign the receipt. The responsibilities for the product will be transferred to merchant.

4. Open the box of device, and check the integrity of the device:

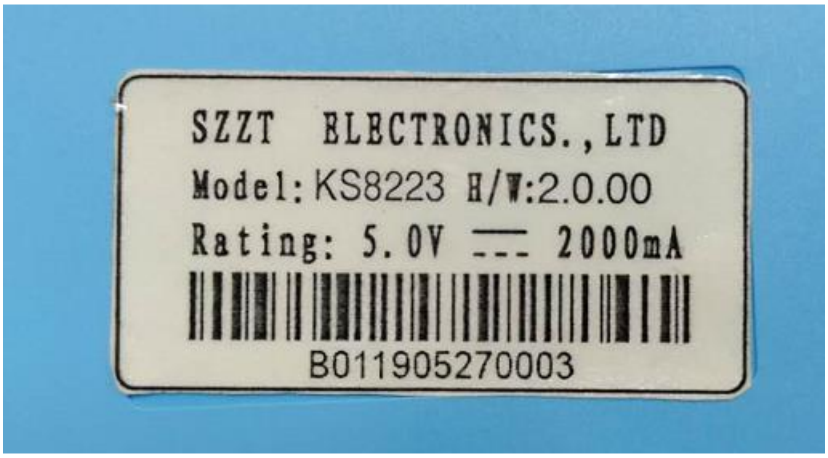
1) Check the tamper-evident label is not ripped off or broken.
2) Check the outward appearance is exactly the same as the picture below:

3) Check the device including the model and logo is intact.

4) Check the hardware version is labeled on the backside of the device, and the software version is shown after powering on the device.

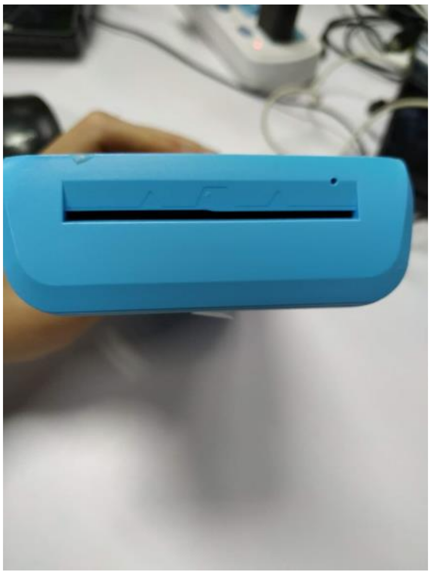


firmware:v1.6.1.13
uboot:v1.0.0
kernel:3.10.49
Android:7.1
Main app:v1.0.0

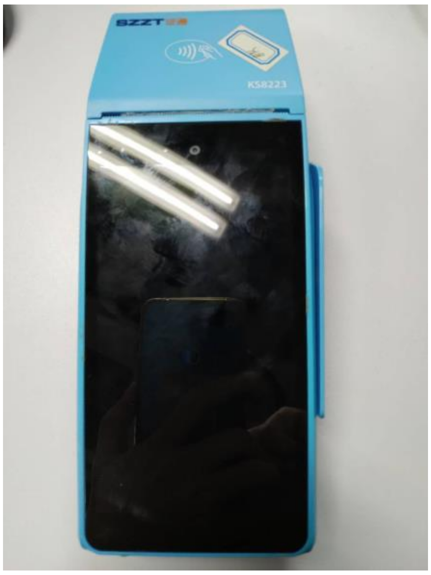


SZZT ELECTRONICS.,LTD
Model: KS8223 H/W:2.0.00
Rating: 5.0V ⎓ 2000mA
B011905270003

5) Check the ICC slot, and make sure there is no any obstruction in it.



6) Check that there are no obstructions in the magnetic stripe card swipe track:



7) Check the accessories are complete, such as the adapter, data line, operation manual

including precautions& security use and so on.

5. Check the screen if there i any suspicious coverings.

2.2 Installation

Handheld devices need not be installed. Equipment needs to be used in good environment. Check the temperature, humidity, clean lines and the power supply are in the reasonable range. Check there is no other sources of interference around the device, like strong magnetic field and so on. Make sure the device works in a good environment. The device is approved as handheld PED product under PCI-PTS 5.1 requirements.

2.3 Environmental Conditions

The ranges of operating temperature, voltage and humidity about the KS8223 are shown as below.

Environment Factor	Minimum Value	Nominal Value	Maximum Value
Voltage	3.4±0.1V	3.7 V	4.2±0.1V
Working Temperature	-10°C		50C°
Storage Temperature	-20°C		80C°
Working Humidity	10%		90%
Storage Humidity	5%		95%

2.4 Communications and Security Protocols

The following describes the communication methods and security protocols available in the device. Use of any method not listed in the security policy will invalidate the PCI PTS approval of the device.

	Interface	Security Protocols
Communication	Cellular Modem (2G,3G,4G)	TLS1.2
	Wi-Fi	TLS1.2
	USB	N/A

2.5 Configuration Settings

1、Enter the system at the first time: Administrators' passwords must be modified after powering on the device for the first time.

Log in with the default password firstly, and then the administrator must re-set a valid password to replace the default password so that the device can be used continuously. Two administrators' passwords are needed to input correctly, then the device can be run in the key-loading status when the device run for the first time. The administrator gets five login attempts to enter the correct password. If this value is reached, the device will be locked, and can't run any more.

Note:

The default password of device for administrator A is "11111111", and for administrator B is "22222222".

What is more, the new passwords cannot be the same as the default passwords.

2、The application keys must be downloaded into device when the device run for the first time.

PIN key initialization is managed by the acquirer. For more details, see the step 4.

3、Not run for the first time: The device enters the normal state. In normal state, the functions include running the applications and entering system menu. The system menu contains the functions of loading the applications and application keys, setting and testing the WIFI, changing the password, and checking the version.

4、After the device was shipped out, and has not yet been installed in merchant, the device should be sent to the acquirer to do the key initialization and replace the authentication and master keys which were loaded by vendor before shipment. The loading of keys must be done under dual administrators' control. Only inputting two administrators' passwords correctly, can enter the status of downloading keys. There is a time limit of 15 minutes in the whole key-loading process. If the key-loading is not finished in 15 minutes, the device will return to the normal status, and if wrongly inputting the passwords over five times, the device will be locked, and provide no service. After finishing the key initialization, the device will be installed in merchant to be used.

5、The details of downloading the keys is as follows:

When downloading application keys to KS8223 device, input two administrators' passwords, and input PTK, then download the keys into device.

2.6 Handheld devices

For handheld devices:
When using the IC reader, if the transaction requires IC card, the checking of the ICC slot in

the device must be done first:

1. Tilt the device a little angle to view the inside of the IC card slot. If there is any abnormal object inside, the device can't be used.
2. Insert an IC card into the slot (insert the IC card with the chip upward), check if the card is inserted smoothly, without any obstacles.
3. Hold the device and enter a PIN as described above to complete the transaction.

When the user is going to enter the PIN, he (or she) should be told to do as above to protect the inlet. Carefully check whether the screen is covered.

3. Operation and Maintenance

3.1. Periodic Inspection

The device must be inspected every day, as follows:

1. Environment checking

Check the temperature, humidity, cleanliness and the power supply are in the reasonable range. Check there is no other sources of interference around the device, like strong magnetic field and so on. Check the tamper evidence physical seals, make sure they are intact. Please refer to section "Tamper Response" for more information. Make sure the device works in a good environment.

2. Device checking

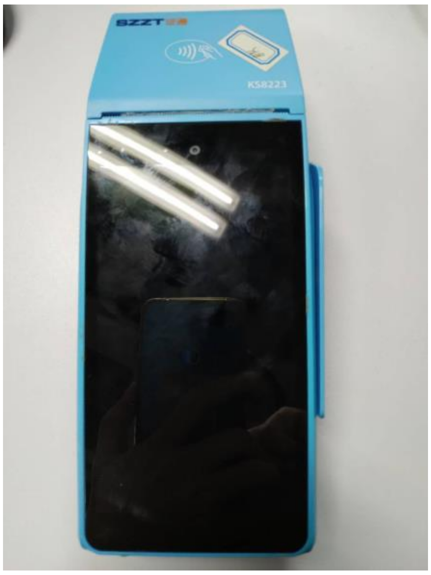
Check the hardware, serial cable and the body of the device. Make sure the case and whole device are intact.

3. Overlay detection

Check the screen if there is any suspicious coverings.

4. Obstacle check

Check the IC card slot and magnetic stripe card swipe track for obstructions.



3.2. Self-Test

The device must perform a self-test at startup, and then perform at least once every 24 hours.

The self-test includes:

- Check firmware integrity and authenticity
- Check application integrity and authenticity
- Check installed keys' integrity

If any of the above check fails, the device will be invalid automatically and can't be used. In this case, please contact the supplier center.

For more details, please refer to "self-check design[v1.0].docx".

3.3. Roles and Responsibilities

The customers of the vendor are acquirers. Vendor sells devices to acquirer and provides maintenance and technique support. Acquirer sells devices to the end-users and services to the end-users. Vendor, acquirer and end-users play different roles in operating device as shown below

Acquirer: 1. Organize the third party to develop application.
2. Download application and import customer key
3. Access to device sensitive services

End-users: Perform transaction.

Vendor: 1. Download initialization key.
2. Sign customer keys.
3. Repair devices and unlock the devices if be tampered.
4. Download key.

3.4. Passwords and Certificates

Enter the system at the first time: administrators' passwords must be modified after powering on the device for the first time.

Log in with the default password firstly, and then the administrator must re-set a valid password to replace the default password so that the device can be used continuously. Two administrators' passwords are needed to input correctly, then the device can be run in the key-loading status when device run for the first time. The administrator gets five login attempts to enter the correct password. if this value is reached, the device will be locked, and can't run any more.

Note:
The default password of device for administrator A is "11111111", and for administrator B is "22222222".

What is more, the new passwords cannot be the same as the default passwords.
The application certificates must be downloaded into device when runs in the first time.

3.5. Tamper Detection and Response

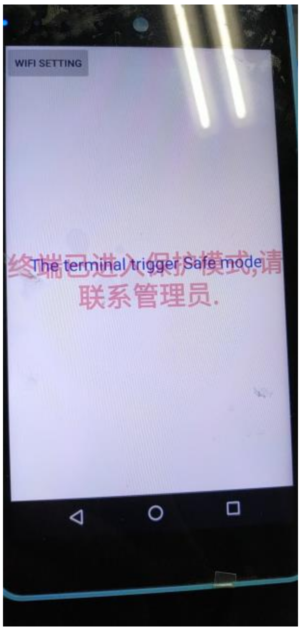
3.5.1 Tamper Trigger Events

- ➢ Front case removal
- ➢ Back case removal
- ➢ Physical penetration on all the sides of the device

- MSR head cover removal
- MSR connector removal
- Temperature is >120C° or <-60C°
- Security processor backup battery voltage is outside of range, approximately <2.1V or >3.8V;
- Stored sensitive data authentication failed during the Self-test

3.5.2 Tamper Response

Remove the stored key file.
The device stops responding and return device to vendor for repair.
After triggering, it is shown as follows:



The terminal trigger Safe mode

终端已进入保护模式,请联系管理员.

3.6. Privacy Shield

The following table shows the combinations of methods that must be used when installing the KS8223 Series terminal to protect the cardholder's PIN during PIN entry.

Method	Observation Corridors				
	Cashier	Customer Queue	Customer Elsewhere	On-Site Cameras	Remote Cameras
Countertop with Swivel Stand	No Action Needed.	Customer positions PED.	No Action Needed.	Do not install within view of cameras.	Do not install within view of cameras.

Countertop without stand	Position unit to face away from the cashier. Use signage to block cashiers view.	Position unit between customer and the next in cue. Install the optional privacy shield.	Used the body to block the view of other customers and the device.	Do not install within view of cameras.	Do not install within view of cameras.
Customer Instruction	Used the body to block the view of the cashier and the device.	Used the body to block the view of other customers and the device.	Used the body to block the view of other customers and the device.	Do not operate within view of cameras.	Do not operate within view of cameras.

Note: The stand swivels to allow the cardholder to position the PED to optimize their viewing angle. If the stand will be used, you must include prompts in your application directing the cardholder to position the PED strategically to restrict the view of other.

Additionally, you may wish to implement the following to further increase security during PIN entry.

- Offer PIN security literature at the point of sale.
- Use signage to limit the view of the PED to just that of the cardholder.

When the user is going to enter the PIN, he (or she) should be told to do as follow to protect the inlet.

Carefully check whether the screen is covered.

The user should cover the soft keypad area with one of his (or her) hands during entering the PIN.

In this way, the number area will not be seen except by the user. It can protect the user’s secret code from peeping by the others when entering.

The vendor has added customer instructions into the cardholder user manual, to introduce to cardholder how to use another hand to prevent the PIN inputting disclosed from any directions.

3.7. Patching and Updating

If the device in the field needs to update the version of firmware or application, the vendor can push the OTA upgrade package to it or the device can be sent back to vendor to do the upgrading process.

The steps are as follows:
For the firmware:

Step	Description
1	Vendor releases new version of firmware, and makes the OTA upgrade package. Use the vendor KSM to make the signature.
2	Acquirer receives the notification of updating the firmware. Connect the device to the network.
3	Vendor pushes OTA update packets through the network (TLS protection), and PDA automatically downloads OTA update packets after receiving the push.
4	After downloading the OTA update package, check the signature. If correct, prompt the acquirer to confirm the update, check the failure, and delete the downloaded OTA update package.
5	After confirming the update, the PDA enters recovery mode, performs the update action, prompts the update progress, and automatically restarts after the update is completed.
6	After the update is completed, the acquirer checks the relevant version information.

For application:

Step	Description
1	The application developer releases new version of PDA application, and uses the KSM (Signature tool) to make the signature.
2	The administrators of the acquirer will download the PDA application to the device following the operation manual that provided by vendor. Put the signed application files into SD card and install SD card to the device. The signature of application will be checked, only legal application will be checked ok and saved to device. Illegal application will be refused. When downloading an illegal application, the PDA will prompt and delete the corresponding legal application already saved in the device.

3.8. Decommissioning

The device’s lifetime is about five years.

3.8.1 Permanent removal

When the device reaches its lifetime or any other reason for no longer use, the device administrator shall remove all the keying material that used to decrypt any sensitive data from the device, so that the device will be permanently decommissioned and removed from service. It can be done by directly disassemble the device to make the device tampered.

3.8.2 Temporary removal

If the device is temporarily decommissioned, all sensitive data are kept and protected by battery power supply, no any operations for change state of device are needed.

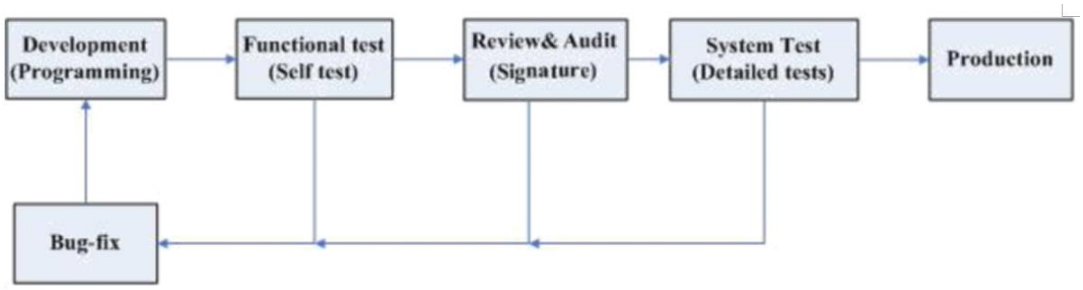
4. Security

4.1 Software Development Guidance

When developing applications, the developer must follow the guidance described in the document "OP secure software development guide".

4.1.1 The development process

During the software development, the following steps must be implemented:


Development (Programming)
Functional test (Self test)
Review& Audit (Signature)
System Test (Detailed tests)
Production
Bug-fix

1.Software development/programming should accord the requirement;
2.After the software development, developer must take functional test (self-test);
3.Take the code review, audit, and digital signature;
4.Undergo a full testing (detailed test);
5.If some bugs are found, the tester will feed back to the relevant developer to fix up;
6.Only after the tests are passed, can the software be released to production.

4.1.2 SSL/TLS application development

The device does not support SSL. For SSL/TLS application development and the compliance with PCI PTS, the following points need attention.
1.The client must authenticate the CA authentication and client authentication.
2.The cipher suite of the server which terminal connects should be as secure as TLS_RSA_WITH_AES_128_CBC_SHA or securer.
3.The server which terminal connects should be configured to require Client authenticate.
4. Use TLS v1.2 or higher. Use other version protocols will violate the PCI PTS approval of the device.
5.Application developer must use SHA-256 on top of the security

6.Protocol when it is being used for security functionality.

For more information, you can refer to the 4.2 chapter or document "OP secure software development guide".

4.2 SSL/TLS

Because of the inherent weakness of SSL, we have removed SSL from the device.
The KS8223 supports WIFI and Cellular(2G/3G/4G) module, in the process of transaction, communication between the KS8223 and server through WLAN or Cellular(2G/3G/4G). In order to make sure the communication is under security control, the KS8223 must connect to the legal server and send the cipher text to the server. Then there needs a mutual authentication between device and server, and the message transmitted to server must be encrypted, in order to make sure the transaction can't be monitored by illegal server, and the transaction data can't be got by hackers.

Using the mutual authentication mechanism of the OpenSSL to make sure the security of communication between KS8223 and server. The public and private keys used in the process of mutual authentication are generated by OpenSSL, which are got from the official website (http://www.openssl.org/source/) of the OpenSSL, and use the latest one "openssl-1.0.2l.tar.gz", which solves all the vulnerabilities found for now (http://www.openssl.org/news/vulnerabilities.html). The TLSV1.2 handshake procedure is described as follow, and the used cipher suite is "TLS_RSA_WITH_AES_128_GCM_SHA256":

The mutual authentication procedure between server and KS8223 terminal is as follows:

1) KS8223 sends the version of its TLS protocol, the type of encryption algorithms, the generated random number and other necessary messages to server.
2) Server sends the version of its TLS protocol, the type of encryption algorithms, the generated random number and other necessary messages to KS8223, also sends its certificate.
3) KS8223 will check the legitimacy of server, including whether the certificate of server is expired or not, whether it's signed by the trustable CA or not, and whether the CA's public key can decrypt the signature in certificate or not. If verify successfully, then the server is legal and continues, otherwise ends this procedure.
4) KS8223 generates a random number as session key, and uses server's public key (got from server's certificate) to encrypt it and sends the cipher text to server.
5) Also, the KS8223 will generate a random number, and sign it using its private key, and send the random with signature and its certificate and cipher session key to server.
6) Server will check the KS8223's certificate and the signed random number's legitimacy.
   For certificate: whether the certificate is expired or not, whether it's signed by the trustable CA or not, whether the CA's public key can decrypt the signature in certificate or not.
   For random number, use KS8223's public key (got from KS8223's certificate) to verify the legitimacy. If one of them verifies unsuccessfully, end this procedure; otherwise,

verifies successfully and server uses its private key to decrypt the encrypted session key, and then generates the finally session key, which is done in KS8223 too.

7) KS8223 and server use the same final session key to encrypt the data transmitted between KS8223 and server, also the integrity of the data must be sure to avoid to be modified.
8) KS8223 sends message to server, tells sever the final session key which will be used to be the symmetry key, and informs the server to end the handshake.
9) Server sends message to KS8223, tells KS8223 the final session key which will be used to be the symmetry key, and informs the KS8223 to end the handshake.

   Mutual authentication is successful and done. The secure channel is built between KS8223 and server, then the data encrypted by the symmetry key can be transmitted between KS8223 and server, also the integrity of the transmitted data will be checked.

In actual use environment, the KS8223 is used as a client, processes the transaction and sends the transaction data to the server. The main protection is for the transmitted data to make sure the communication channel between device and server is security, the data will not be sent to illegal server, and the plain text of the data can’t be intercepted and illegally modified.

Reference document "OP secure software development guide" can provide more details.

4.3 Signing

4.3.1 Applications and firmware downloaded to the device must be signed to install.

4.3.2 Signature algorithm:

1) APP: SHA-256 and RSA (2048)
2) AP firmware: SHA-256 and RSA (2048)
3) SP firmware: ECDSA -256 and SHA-256(2048)

4.3.3 When download application, the device will authenticate the signature of application. Only authenticate successfully, the application can be installed.

4.4 Account Data Protection

Use algorithms: TDES (192bits).

Account data (For example: PAN, expiration date, etc.) read from IC, contactless card, and magnetic stripe card must be encrypted at once. The plain-text account data cannot be output from the device. After transaction finished or time out or other abort, the plain-text account data must be deleted immediately.

Device does not support closing account data encryption.

4.5 Algorithm Supported

KS8223 supports the following cryptographic algorithms:

1.TDES (128bits, 192bits)
2.AES (128bits, 192bits)
3.SHA-256(digest signature, 256 bits)
4.RSA-2048(signature verification, mutual authentication,2048 bits)
5.ECDSA-256(firmware verification,256 bits)

4.6 Key Management

The terminal device implements MK/SK, Fixed key and DUKPT key management techniques:
1.Master Key / Session Key: a method built based on a hierarchy of keys. The session keys are unique per transaction as specified in [6.2].
2.DUKPT: a key management technique based on a unique key for each transaction as specified in [6.3].
3. Fixed key: Fixed key refers to AES key, which is downloaded in clear text under dual control in secure environment and saved in SP internal flash.
Attentions:
Use of the POI with different key-management systems will invalidate any PCI approval of this POI.

KEY TYPE	Purpose	Algorithm	Size(bits)	Storage
AESK	Used to encrypt/decrypt the data stored in NVSRAM by SP's hardware automatically	AES	256	SP secure key register
MK	Master key which is used to encrypt PINK, MACK and DESK (MK/SK)	TDES	128/192	SP's inner Flash.
PINK	PIN block encryption key for format 0 (MK/SK)	TDES	128/192	SP's inner Flash.
MACK	Message authentication key (MK/SK)	TDES	128/192	SP's inner Flash.
DESK	Account Data encryption key (MK/SK)	TDES	192	SP's inner Flash.
FPINK	PIN block encryption key for format 4 (Fixed)	AES	128	SP's inner Flash.
PTK	Used to encrypt key data during key injection	TDES	192	Temporarily stored into SP's inner RAM during key loading, and cleared immediately after key loading.
MMK	Used to encrypt the keys	AES	192	SP's NVSRAM

	stored in the SP’s Flash and AP external Flash			
DUKPT initial key	Used to generate the DUKPT Current Transaction Keys	TDES	128	Designated Key Register
DUKPT Current Transaction Keys	Encrypt MAC or PIN for security	TDES	128	Designated Key Register
ELRCK	Used to encrypt the checksum values of the keys stored in the SP’s Flash and external Flash	TDES	128	SP’s NVSRAM
LSK-PUB	The public key to verify the signed MSM8909’s LK(Little Kernel)	RSA	2048	Compiled into firmware
KSK-PUB	The public key to verify the signed MSM8909’s Kernel	RSA	2048	Compiled into firmware
RSK-PUB	The public key to verify the signed MSM8909’s System	RSA	2048	Compiled into firmware
Certificate of CA RSA public key for OP	Used for authenticate the legitimacy of KS8223 when mutual authentication between KS8223 and server	RSA	2048	Compiled into firmware.
RSA public and private key for OP	Used for mutual authentication between POI and server during communication and data transmission.	RSA	2048	AP’s external Flash.

4.7 Key Loading

Before downloading application keys to KS8223 device, two administrators’ passwords and PTK should be input. Then download the keys into device.

About key loading, we use KSM to download application keys into device under dual control in secure room. The KSM was placed in secure room, where only the administrators have the authority to enter into. When the device needs to download keys, the administrators take it to secure room. Before using the KSM to download the keys into device, the administrators’ passwords must be input right.

4.8 Key Replacement

There are symmetric master keys used in the device, for some secure reason, like the crack technique is improved day by day. Once the keys are cracked by hacker, the device is not security any more. So the keys saved in the device must have a life cycle, usually a year for symmetric master keys. Another case: once the compromise of the original key is known or suspected, the key must be replaced with a new key immediately.

To replace the key through external selection, the key index and key type must be specified. Only the key with the same index can be replaced. However, the replacement of application signature key must input PCK check.

5. Acronyms

Abbreviation	Description
PCK	Public Check Key
PDA	Personal Digital Assistant
KSM	Key System Management
PCI	Payment Card Industry
PTS	PIN Transaction Security
PIN	Personal Identification Number
KLD	Key Loading Device
DES	Data Encryption Standard
TDES	Triple Data Encryption Standard
RSA	Rivest/Shamir/Adelman Algorithm
IC Card	Integrate Circuit Card
HW	Hardware

6. References

[1]PCI PTS POI Modular Derived Test Requirements Version 5.0 - Sept 2016

[2]ANS X9.24-1:2009, Retail Financial Services Symmetric Key Management Part 1: Using Symmetric Techniques

[3]X9 TR-31 2010, Inter-operable Secure Key Exchange Key Block Specification for Symmetric Algorithms

[4]ISO 9564-1, Financial services-Personal Identification Number (PIN) management and security — Part 1: Basic principles and requirements for PIN in card-based systems

[5]ISO 9564-2, Banking-Personal Identification Number management and security Part 2: Approved algorithms for PIN encipherment

[6]KS8223 OP secure software development guide